ECDL Foundation

IT SECURITY SKILLS

PROTECTING YOUR CHILDREN, YOUR PRIVATE LIFE, AND YOUR BUSINESS

Contents

ECDL Foundation is a stakeholder in the eSkills for Jobs campaign, an initiative of the European Commission

INTRODUCTION

With the number of cyber security breaches increasing every year, their scale and costs grow exponentially[1]. Methods of illicitly gathering information, for example, phishing, spamming, and hacking, are becoming more sophisticated, and protecting information online is thus becoming increasingly important. This paper discusses the IT security needs in private and professional spheres, and provides examples of cases where cyber security principles were not followed. The paper suggests that even the most advanced IT security products cannot solve the problem alone: people need greater awareness and the right skills to protect both their own data, and their company's data.

1 ENISA, Cyber 7, 2015, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/cyber-7-seven-messages-to-the-edge-of-cyber-space

1. Private Life Needs to be Protected

Everyday life is increasingly becoming digital. In Europe, 65% of internet users already order goods and services online, 63% participate in social networks, 57% use online banking, and 13% make appointments with health practitioners online[1]. These activities make life easier, but also raise additional security concerns. Awareness of possible threats and an understanding of how to protect personal data and stay safe online are crucial. Yet, just under half of EU citizens feel well informed about the risks of cybercrime[2]. As the case of Mat Honan shows, negligence of simple cyber security principles in private life might be disastrous.

Mat Honan, a technology journalist in San Francisco, had all of his digital accounts hacked and compromised within one hour[1]. First, hackers got into his Amazon account and altered his personal data, which allowed them to get access to his Apple ID account. Having done that, they erased all the data from Mr Honan's iPad, iPhone and MacBook, including irreplaceable pictures of his family and the first years of his child. Then, criminals connected to Mr Honan's Google account and deleted it. Finally, they reset his Twitter password and used it to broadcast racist and homophobic messages.

Mat Honan admits that it was partially his fault, as all of his accounts were closely related to each other. Harsh consequences could have been prevented had he taken some simple security steps such as backing-up the pictures he kept online and using a two-factor authentication process for his Google account.

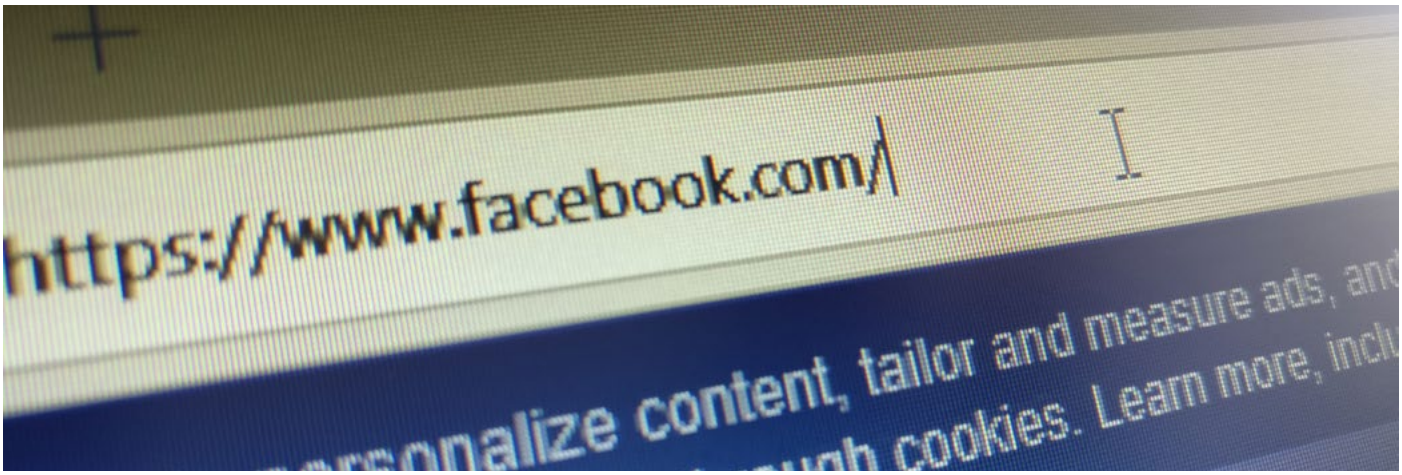
1 Mat Honan "How Apple and Amazon Security Flaws Led Me to My Epic Hacking", http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

1 European Commission, Digital Scoreboard, https://ec.europa.eu/digital-single-market/en/create-graphs
2 Eurobarometer "Cyber Security", 2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

2. Children and Young People Are Particularly Vulnerable Online

Children and young people are among the most vulnerable groups online. Despite the widespread illusion that young people are 'digital natives' and therefore use digital technologies safely and efficiently, various studies show that this is not the case[3]. For example, the Net Children Go Mobile survey shows that around half of all 11-16 year olds have encountered one or more risks on the internet and that the proportion of children who report being bothered or upset online has increased in recent years[4].

A survey of Italian university students revealed that most of them have very low digital security skills. For example, 42% of the students are not adequately aware of the risks of using free Wi-Fi, 40% of them do not protect access to their phones, and 50% of students never, or rarely, control permissions that applications require before installation[5]. Young people also tend to share a wide range of private information on-line, which they often later regret[6]. Most of these online threats could be prevented if young people were taught early on about the essentials of IT security.



Highlighting the dangers that poor internet security skills can present, Panorama[1], a Belgian television programme invited a recruiter from recruitment agency, Randstad, to demonstrate how an employer might find information about students. She searched for photos of one of the students on Facebook, with the first result being a photo of the girl in a hot-tub that had been posted by her mother. The girl was shocked to see the photo appear in public results. She had tried to be careful with her sharing settings, but because her mother was able to tag her in the photo, she had little control over the types of photos that potential employers might see when she applies for a job. By simply activating a setting that would allow her to approve when she is tagged by others, she could have avoided the surprise and potential embarrassment from very personal photos being posted online.

1 VRT, Panorama, http://deredactie.be/cm/vrtnieuws/videozone/programmas/panorama/2.27142

3 More information about digital skills of young people can be found in ECDL Foundation position paper "The Fallacy of the 'Digital Native': Why Young People Need to Develop their Digital Skills', 2015, http://www.ecdl.org/media/TheFallacyofthe'DigitalNative'PositionPaper1.pdf

4 Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile, 2014, http://eprints.lse.ac.uk/60513/

5 Tech and Law Center, "Security of the Digital Natives", 2014, Italy.

6 http://ikeepsafe.org/be-a-pro/reputation/hey-teens-chances-are-youll-regret-oversharing-personal-information-online/

3. To Prevent Losses, Business Needs to Adapt

Cyberattacks on business have become more frequent in recent years. For example, in 2015, nine out of ten large organisations in the UK reported having experienced an information security breach[7]. Potential damage for companies includes the loss of intellectual property, sensitive business information and confidential client data, a decrease in consumer confidence and reputational damage. It is estimated that for companies that employ over 500 people, the average cost of the most severe online security breach is between €2.03 million and €4.38 million[8].

The entire business of a vehicle hire company, MNH Platinum, was threatened in 2015 when one of the employees clicked on a suspicious email link. The company's network was attacked by a virus which encrypted over 12,000 files that were vital for the company's work. The attackers demanded a ransom of more than €4,000 (about £3,000) in exchange for decrypting company's files. To get the crucial data back, the company had no choice but to pay the demanded money to the criminals.

"We were completely unprepared for a cyber breach simply due to a lack of awareness of the magnitude an attack of this type could have through mistakenly clicking a link in an email," said managing director Mark Hindle. "I am thankful that we had a lucky escape, in that I was able to retrieve the documents that are crucial to the running of the business, albeit at a price."[1]

MNH Platinum would had never faced such a danger for its business if its employee, who clicked on the link, had had a better understanding of cyber security threats.

1 Mark Smith, "Huge Rise in Hack Attacks as Cyber-Criminals Target Small Business", 2016, https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses

Small and medium businesses (SMEs) are particularly sensitive to IT security breaches. SMEs often naively assume that they will not be threatened online. In fact, SMEs are more likely to be targeted because they tend to have weaker defences due to a lack of human and financial resources[9]. The Information Security Breaches Survey 2015 revealed

7 2015 Information Security Breaches Survey, http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

8 Originally – between £1.46 million and £3.14 million. Currency converted from British pounds to Euros for the approximate date of publication of the study – June 2015. 2015 Information Security Breaches Survey, http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.

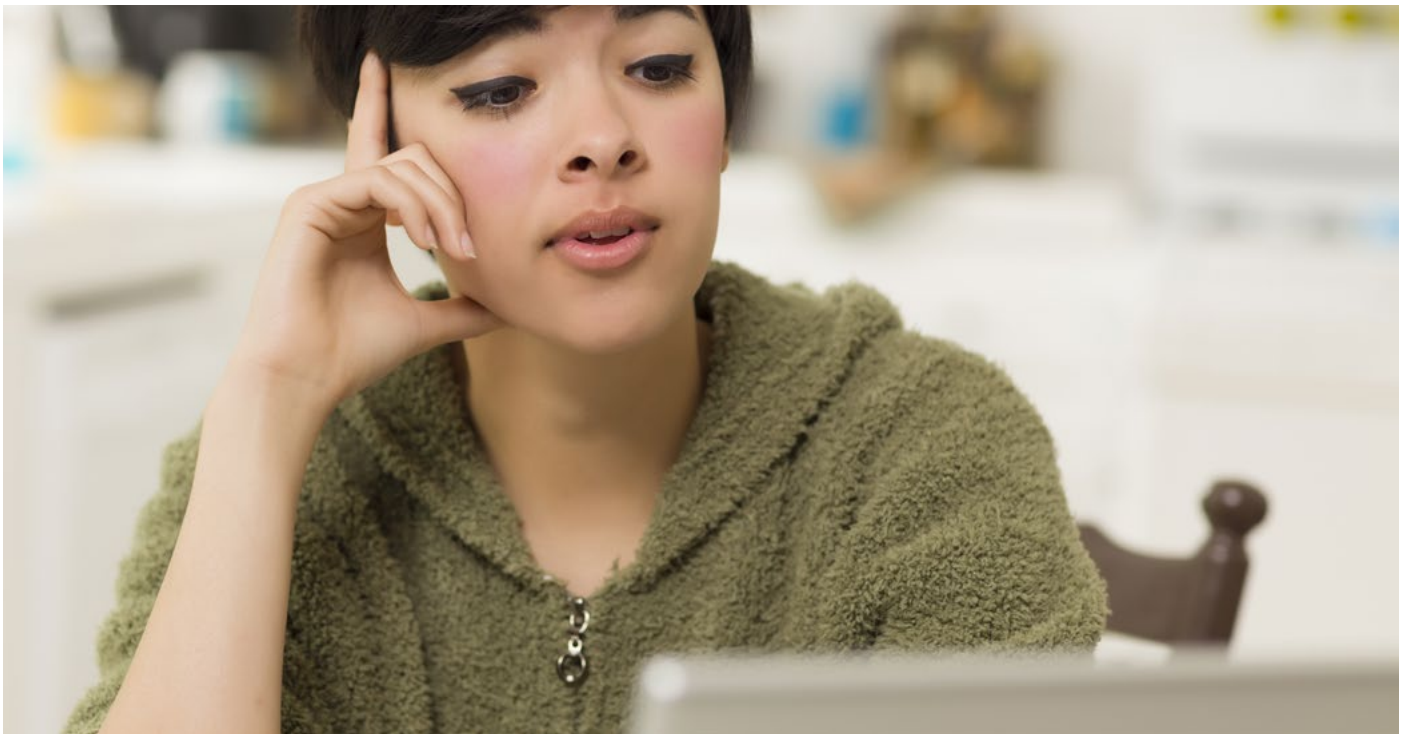
9 Mark Smith, "Huge Rise in Hack Attacks as Cyber-Criminals Target Small Business", 2016, https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses

that nearly three-quarters of SMEs had suffered a security breach in the last year and that the average cost of the worst breach was from €104,500 to €433,160[10].

4. Humans are More Vulnerable than IT Systems

The vendors of IT security products – anti-virus, anti-spyware, etc. – can sometimes suggest that their products will, in a fully automated fashion, tackle all internal and external security threats. However, the technologies intended to provide security ultimately depend on their effective implementation by people.

A usual mistake that organisations make is trying to minimise security risks by applying very stringent IT security measures to internal networks, and by implementing seemingly exhaustive security policies for employees. These policy measures, while effective, cannot by themselves wholly eradicate IT security threats. While it is extremely rare that employees intentionally set out to sabotage or endanger employers' networks and operations, the IT security measures outlined above do not always ensure that well-meaning employees don't inadvertently compromise the security of their organisation through seemingly harmless actions.



Cyber security literature admits that people are the weakest link in any security chain[11]. A substantial number of online security breaches occur because a company's employees simply click on suspicious links, download unauthorised software, or access websites that could compromise networks. Most of these situations could be prevented if company employees had the right skills and knowledge to recognise cyber threats and avoid them. The UK Government estimates that seven out of ten cyber-attacks could be prevented[12] if companies followed the right security measures.

10 Originally - from £75,000 to £310,800. Currency converted from British pounds to Euros for the approximate date of publication of the study – June 2015. 2015 Information Security Breaches Survey, http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.

11 Mark Smith, "Huge Rise in Hack Attacks as Cyber-Criminals Target Small Business", 2016, https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses

12 "Cyber attacks: Two-thirds of Big UK Businesses targeted", 2016, http://www.bbc.com/news/uk-36239805

5. IT Security Skills Are Crucial to Staying Safe Online

Investing in IT security products will never ensure full protection if not accompanied with the right IT security skills and a good understanding of cyber threats. Only by understanding and being able to identify the main concepts underlying the secure use of ICT in daily life, and by having the necessary skills and knowledge needed to maintain a secure network connection and use the internet, will the user be able to protect their data – and that of their company – from being compromised.

One way of establishing good IT security practices for the individual, and by extension for the organisation, is by implementing recognised training programmes and certifications that benchmark the user's levels of skills and knowledge against an internationally recognised standard.

6. Development of IT Security Skills – ECDL Foundation Perspective

IT Security Module Version 1.0

In 2010, ECDL Foundation developed a specific module relating to IT security[13]. The main drivers behind this were a demand from ECDL Foundation National Operators for a user-focused, as opposed to a practitioner-focused, certification. In tandem with this was an increased awareness of IT security by both organisations and policy makers. ECDL Foundation decided that a separate certification solution would allow for a deeper and broader engagement with the issue of IT security that could move beyond awareness and focus on conceptual knowledge and practical skills.

The IT Security Module Version 1.0 was launched in 2010. The Module set out essential concepts and skills relating to the ability to understand the main concepts underlying the secure use of ICT in daily life and to use relevant techniques and applications to maintain a secure network connection, use the internet safely and securely, and manage data and information appropriately.

13 ECDL Foundation uses the following development process of its modules: first, it draws on the expertise of its network of National Operators, which includes the computer societies of Europe. This expertise is crucial to identify the essential knowledge and skills that should be included as learning objectives in its certification modules. In addition, these National Operators run networks of test centres. These test centres are not just crucial in deploying the programme – they are also very valuable in identifying the correct skills and knowledge for a particular domain, such as IT security

IT Security Module Version 2.0

In 2014, ECDL Foundation decided to update the IT Security module to ensure that the content was reflective of some of the emerging and most crucial trends in this topic area. In particular, consideration is given to issues relating to the emergence of the cloud as a location for data and services, secure use of social media, and the ubiquitous use of mobile devices.

The module[14] is aimed at anyone who needs to understand concepts relating to the secure use of ICT in daily life and to apply skills in order to maintain a secure network connection, use the internet safely and securely, and manage data and information appropriately. Individuals who wish to protect their own data and digital identity, as well as employees who need to protect their organisation's data, can benefit from this module.

Uptake of the Module

To date, the uptake of the IT Security module has been very positive. For example, in 2015, approximately 93,000 IT Security tests were taken by candidates globally, demonstrating the relevance of this module for individuals who are developing their digital skills using the broader ECDL programme.

'Click safely! You can with ECDL – Protect yourself with IT Security'[15] is a programme which started in Italy in 2015. It aims to provide all high school students with the competences necessary to surf and use the web in a safe and aware way. Building on a relationship between AICA, the ECDL National Operator in Italy, and the Ministry of Education, this programme raises students', parents' and teachers' awareness of the safe use of new technology and mobile devices. The programme is available to approximately 3 million Italian high school students, who can access an e-learning programme and proceed to formal certification of their skills if they wish.

14 ECDL Foundation "IT Security", http://www.ecdl.org/programmes/media/ECDLITSecurity_Syllabus2.01.pdf
15 AICA, http://www.aicanet.it/iocliccosicuro

CONCLUSION

Ultimately, it is the actions of the human user that increase the level of exposure to IT security breaches. Installing the most heightened automated security measures and prescriptive policies is only a partial solution. Most of the cyber security breaches could be prevented and high costs avoided if people followed simple IT security principles like using secure passwords, installing anti-virus and anti-malware software, not disclosing confidential or personal identifiable information on social networking sites and not clicking on suspicious links.

Children and young people are extremely vulnerable online. They should be empowered to protect themselves from a very young age so they can enjoy the benefits of digital life. Ideally, all primary and secondary school students should receive training on the risks and safe use of the internet.

The costs inflicted by cyber security breaches might be significant for business. To avoid potential losses, companies should make sure that their employees are properly trained and aware of the on-line risks.

To improve and maintain IT security both on an individual and organisational level, the awareness levels and behaviour of the user must be positively influenced. Skills and knowledge development programmes that are focused on the most important and current IT security threats are the best tools for achieving this aim.

ABOUT ECDL FOUNDATION

ECDL Foundation is an international organisation dedicated to raising digital competence standards in the workforce, education and society. Our certification programmes, delivered through an active network in more than 100 countries, enable individuals and organisations to assess, build and certify their competence in the use of computers and digital tools to the globally-recognised ECDL standard, known as ICDL outside of Europe.

As a nonprofit social enterprise, ECDL Foundation benefits from the unique support of experts from national computer societies and partners worldwide to develop vendor-independent standards which define the skills and knowledge required to use digital technology effectively. We work with education and training partners, local and regional authorities, national governments, international development organisations, as well as public and private sector employers in all sectors, in the delivery of our programmes.

The quality and reputation of ECDL is built on almost twenty years of experience in delivering our certification programmes to over 14 million people and in more than 40 languages worldwide, with more than 2.5 million ECDL tests taken annually. Our success is maintained by our ongoing innovation in certification programme development, our commitment to rigorous test design methodologies, and consistent adherence to our quality assurance standards.

ECDL Foundation supports the initiatives of National Operators of the programme in Europe and the Arab States from our headquarters in Dublin, Ireland and our European office in Brussels, Belgium. We have also established three regional operations – ICDL Africa (based in Rwanda), ICDL Asia (based in Singapore) and ICDL Americas (based in Panama). All ECDL Foundation operations work closely with regional, national and local partners to develop the global network of ICDL Accredited Test Centres.

ecdl.org